DAPSCOIN

DECENTRALIZED-ANONYMOUS-PAYMENT-SYSTEM

WHITEPAPER
2019

«Privacidade é um direito, não um privilégio»

INTRODUÇÃO

DAPS é uma blockchain de privacidade com foco em segurança, escalabilidade e privacidade total. O objetivo do protocolo DAPS é criar um sistema de pagamentos e moedas totalmente anônimos, com uma estrutura de governança “sem confiança” (trustless), com base nas mais recentes tecnologias derivadas da Monero e da PIVX, pela primeira vez. Os modelos de verificação e consenso da rede DAPS serão baseados em nós PoS (Staking e Masternodes), bem como mineradores PoA (Proof of Audit).

Como faremos isso? Selecionamos cuidadosamente alguns protocolos já testados e a utilização desses recursos juntos nos permitirá rodar uma blockchain totalmente privada. Objetivamos oferecer o pacote de anonimato mais completo em qualquer protocolo já visto até o momento, com uma solução dentro de nossa rede para o "Problema da Confiança" – discutido à seguir. Nossa solução exclusiva para o "Problema da Confiança" é chamado Prova-de-Auditoria (PoA), que é o ponto alto do nosso protocolo.

Um dos principais objetivos da DAPS é anonimizar os ativos e garantir infra-estrutura para o desenvolvimento de novas tecnologias à partir dela. Privacidade é um direito, não um privilégio.

DAPS tem o orgulho de informar que, no momento em que escrevemos este whitepaper, somos a primeira moeda a implementar com sucesso uma rede completamente privada e híbrida, contendo Staking e Masternodes (PoW - PoS - PoA), enquanto também incorporando RingCT e Bulletproofs.

POR QUE DAPS?

Nos blockchains tradicionais e em várias blockchains de anonimato "parcial", os usuários são expostos a análise de dados e ataques mal-intencionados. Muitos ao redor do mundo usam esses dados para explorar e prejudicar usuários de criptomoedas. Nosso objetivo é preservar o direito de todos de controlar suas finanças da maneira que desejarem.

HISTÓRIA DO PROTOCOLO DE HARPÓCRATES (DAPS)

O Protocolo Zerocoin (libzerocoin) é a base para muitas das moedas de privacidade que vemos hoje. Usado por outros projetos para criar ativos de privacidade relativamente seguros e protegidos, esse protocolo é altamente testado e é considerado hoje o padrão para a implementação de privacidade.

Usando essa base de privacidade, muitas moedas se expandiram nos conceitos do protocolo Zerocoin (libzerocoin) de várias maneiras, um exemplo notável sendo a DASH.
A Equipe DASH criou uma nova camada em sua blockchain chamada Masternodes no protocolo do Bitcoin, que é, essencialmente, um nó incentivado que funciona 24 horas por dia, 7 dias por semana, para fortalecer a rede e permitir que recursos adicionais da blockchain sejam implementados. Esses recursos incluem o Instantsend, Privatesend, e permitem que os Masternodes votem sobre propostas, descentralizando a governança da rede, tirando-a das mãos do desenvolvedor.

Já a PIVX, fundiu o protocolo Zerocoin com o protocolo Masternode. A PIVX expandiu esse conceito ao implementar um "Sistema de Recompensas em Gangorra" para Masternodes, com objetivo de privilegiar as recompensas dos Masternodes em relação às recompensas de staking (Prova de Trabalho – PoS – na carteira).

Seguindo a definição do protocolo do Sistema de Pagamento Anônimo Descentralizado - DAP, conforme descrito por Sasson et al (2014), o sistema DAP é descrito como um método de pagamento que permite aos usuários fazer pagamentos diretos e privados entre si, ocultando a origem e o destino do pagamento, incluindo valor do pagamento. Essa abordagem à criptomoeda emprega provas de "conhecimento zero" que impedem a análise de transações ou endereços.

Outra metodologia que se mostrou extremamente robusta e bem-sucedida é a RingCT, implementada pela Monero.
Abaixo está um trecho e um link para o paper – em inglês.

["An obvious way to negate the downsides of the CryptoNote protocol... would be to implement hidden amounts for any transaction" -Shen Noether, Ring Signature Confidential Transactions for Monero]

O PROBLEMA DO BITCOIN

Bitcoin não é anônimo. Por definição, para evitar gastos duplos, o blockchain é totalmente público e visível para qualquer pessoa ou entidade. Isso torna o protocolo do Bitcoin “sem confiança”, ou seja, você não precisa "confiar" em nenhum operador de Bitcoin ou na pessoa que te envia Bitcoin, pois você mesmo pode verificar a rede por meio de terceiros. Você pode facilmente verificar seus próprios saldos e transações em um livro-razão público (explorer). Essa é uma das maneiras pelas quais a rede Bitcoin protege a sua integridade, ao custo de expor completamente os usuários finais à análises e rastreamento. Esta é uma desvantagem das redes "sem confiança" (totalmente transparente): transações, balanços e outros dados são facilmente rastreados e podem ser usados por maus atores. Esta questão levou à ideia de blockchains "privados" a se tornar um foco para o mercado de criptomoedas.

"PRIVACIDADE" E SEGURANÇA

Nem todas as moedas de privacidade são totalmente privadas. Em teoria, em uma rede completamente anônima, não importando o protocolo, os proprietários de carteiras (nós ou Masternodes) podem conspirar fora da rede, em conjunto, para executar seus nós maliciosamente. Isso pode ser desastroso de várias maneiras para qualquer rede e representa um risco de segurança interno ainda maior para blockchains privados, criando continuamente moedas para si em segredo e gastando, sem que o mundo fosse capaz de descobrir isso, pois as transações e os saldos estariam ocultos da visão pública.

Como não seria possível "reverter" essas ações sem causar uma divisão da blockchain, é essencial poder detectar ataques ou conluios à medida que ocorrem. Mas, como você verifica o estado da rede, quando as pessoas que deveriam garantir essas informações têm incentivo para serem desonestas?

A maioria das equipes evita a idéia de blockchains privados devido à inerente fragilidade à exploração delas. Essa capacidade de exploração é causada pela incapacidade de se rastrear o estado e as emissões da rede por um terceiro neutro – caso do Bitcoin, que é público. O exemplo mais proeminente desta fraqueza é a vulnerabilidade constante das redes "Zerocoin minting" e CryptoNote.

O QUE É O "PROBLEMA DA CONFIANÇA"?

Para ser “sem confiança”- trustless, uma terceira parte deve ser capaz de verificar o suprimento da moeda, verificar as emissões da moeda e certificar-se de que os nós não estão sendo usados de forma maliciosa. Nós não acreditamos que confiar na honestidade dos proprietários de nós deve ser o único recurso contra ações maliciosas.

Para as blockchains de privacidade baseadas em Masternodes, um grau de confiança deve ser dado a esses Masternodes, como uma governança central do suprimento de moeda, inflação e outras especificações. Para redes de privacidade que não sejam baseadas em Masternodes usando zk-SNARKs, a rede exige um ritual de implantação complicado, em que uma parte de informações de controle de rede é exposta a um pequeno grupo de membros. Se esses membros não excluírem completamente esses dados (e não memorizá-los), a rede poderá ser totalmente controlada por eles.

Este é o "problema da confiança". Você deve confiar nos nós ou em um grupo de "administradores" e figuras centrais que podem controlar toda a rede por capricho. As iterações atuais em blockchains de Masternodes e blockchains totalmente privados (zk-SNARKs, Ring CT com ofuscação total) divergem do status "sem confiança" dos blockchains públicos.

Muitas moedas não privadas também ignoram completamente essas estruturas de governança e configurações de rede “sem confiança”, declarando-se uma rede totalmente centralizada e com autoridade central.

Acreditamos que essas redes são perigosas para blockchains como um todo e que isto viola os princípios da visão de Satoshi Nakamoto. Nenhuma constituição, acordo ou arranjo escritos por homens podem ser tão seguros quanto os fundamentos de um “livro-caixa” de blockchain garantido por terceiros.

Como vamos abordar essas questões? Nossa “Prova-de-Auditoria” introduzirá a necessária confiança à nossa blockchain, que foi concebida com características de outras moedas de privacidade.

**** Isso permitirá a implementação de blockchains totalmente privados, usando ferramentas disponíveis atualmente eque poderão se expandir para muitas redes existentes.***

O QUE NOS TORNA DIFERENTES?

A ideia de Prova-de-Auditoria e implementação do Protocolo DAPS é chamada de Protocolo de HARPÓCRATES e será um novo padrão da indústria.
Utilizando as seguintes tecnologias principais:

- **Ring CT**
- **Bulletproofs**
- **Endereços Secretos**
- **Transações Secretas**
- **Prova-de-Auditoria**

Conseguimos implementar ofuscação completa de todos os usuários e transações. Esse mix de recursos, com a Prova-de-Auditoria - que chamamos de "O Protocolo de Harpocrates" - cria uma blockchain anônima completamente “sem confiança”, ou seja, sem a necessidade do terceiro verificador.

VISÃO GLOBAL DA DAPS

DAPS é uma blockchain híbrida Proof-of-Work (PoW), Proof-of-Service (PoS), Proof-of-Audit (PoA) focada na privacidade dos usuários. DAPS oferece os seguintes recursos exclusivos:

- Uma blockchain com foco em privacidade que garante que todas as transações do usuário na rede sejam mantidas em sigilo. Isso significa que, apesar de todas as transações do usuário serem totalmente publicadas no blockchain, nenhum terceiro, exceto o remetente e o destinatário da transação, pode observar as informações detalhadas dentro da transação. Especificamente, as seguintes informações são mantidas em sigilo no sistema DAPS:
- Remetente da transação: o remetente da transação é totalmente ofuscado;
- Receptor da transação: fora chaves públicas geradas a cada transação para o receptor na transação, nenhum terceiro poderá identificar o receptor da transação ou o relacionamento entre as chaves públicas do receptor e a identidade do receptor;
- O valor da transação é codificado de forma que nenhum terceiro possa descobrir o valor da transação dentro da transação;
- Um sistema de blockchain híbrido que é composto de diferentes tipos de blocos na mesma rede:
- Os 500 blocos iniciais serão blocos PoW (Prova-de-Trabalho) que serão minerados pelos desenvolvedores DAPS para prover fornecimento inicial, que é declarado neste white paper;
- À partir do bloco 501, o blockchain DAPS se tornará um híbrido de blocos PoS (Prova-de-Serviço) e PoA (Prova-de-Auditoria). Os blocos de PoS serão continuamente minerados pelos nós (carteiras e Masternodes), verificando as transações dos usuários no blockchain DAPS. Um bloco PoS é criado a cada minuto;
- Os blocos de PoA (Prova-de-Auditoria) são minerados aproximadamente a cada hora. Os blocos de PoA são minerados para auditar os blocos PoS, garantindo que o sistema esteja funcionado corretamente, ou seja, dentro das regras de consenso especificadas. Um bloco de PoA deve re-auditar pelo menos 59 blocos de PoS, certificando-se da sua correção. Para este trabalho, os mineradores de bloco de PoA também são recompensados para que continuem a auditar o sistema.

MECANISMOS DE CONSENSO DAPS COIN: MASTERNODES, NÓS DE STAKING E PROVA-DE-AUDITORIA

Os Masternodes DAPS devem conter um saldo de 1.000.000 de DAPS em carteira, um endereço IP dedicado e serem capazes de funcionar 24 horas por dia, 7 dias por semana, sem perda de conexão por mais de uma hora. Os Masternodes serão pagos usando o método gangorra, conforme descrito na próxima seção. Por oferecer seus serviços à rede, recebem uma parcela das recompensas do bloco para manter o ecossistema funcionando. Esse pagamento será em DAPS e serve como uma forma de renda passiva aos proprietários dos Masternodes.

O sistema de Masternodes DAPS é modelado à partir do sistema de Masternodes PIVX. Isso trás muitos benefícios, incluindo prevenção de ataques 51%, a menos que ambas as camadas de Prova-de-Serviço e Masternodes sejam comprometidas simultaneamente.
O SBRS (Sistema de Recompensas em Gangorra) terá recompensas por blocos divididas na razão de 60% a 40% entre Masternodes e Staking (carteiras ou nós), rebalanceando para até 40% a 60% considerando sempre recompensas justas para os investidores.

A verificação da blockchain será feita por meio de Prova-de-Auditoria, Masternodes e Prova-de Serviço (v3). Isso dará à rede DAPS resistência contra os ataques mais conhecidos e garantirá que a rede seja segura, permitindo que ela seja examinada publicamente (emissões e altura dos blocos).

Embora a blockchain da DAPS seja “sem-confiança”, ainda é preciso haver um elemento de confiança.

Masternodes, em qualquer blockchain de Masternodes, são vistos como um nó confiável. Isso se deve à garantia em moedas que estão bloqueadas em suas carteiras, como exigência para que o masternode seja considerado confiável. DAPS é, por definição, anônima, com valores de transações ocultos. Isso representa um problema específico ao colateralizar um Masternode com 1.000.000 de moedas e garantir que a quantia esteja correta e trancada.

Portanto, todas as transações de colateralização para Masternodes têm a quantia visível que não é Bulletproofed nem parte de uma Ring Signature.

Assim que o Masternode é desfeito, o UTXO (transação) que foi usada como garantia, é enviada de volta para a carteira designada e é tratada como uma transação normal – totalmente oculta.

SEGREDO OBRIGATÓRIO

DAPS possui um sistema de endereço secreto obrigatório e todos os valores de transações do usuário são ocultados por meio de codificação. Ao criar uma transação, o remetente gera uma chave pública de transação (1) por UTXO*, que é então usada para gerar uma chave pública única (2) - correspondente a um endereço de Bitcoin, por exemplo. A chave privada desta (2) é então derivada da chave única do receptor da transação, que terá acesso aos gastos ora privados e chaves (descritos mais adiante). Os valores da transação são codificados usando um esquema de criptografia simétrica que usa o ECDH Elliptic-Curve Diffie Helman para codificar os valores das transações, que só podem ser revelados pelo remetente e pelo destinarário da transação. A chave pública da transação permitirá que o detentor da chave privada gerada revele apenas o valor dessa transação. Nenhuma outra transação pode ser revelada com a mesma chave.

*Unspent Transaction Output – Transações não-gastas em carteira (que compõe o saldo positivo dela)

EMISSÕES

As emissões de moedas DAPS serão de 1050 DAPS por bloco. Haverá uma taxa de 50 DAPS por bloco (taxa do fundador) alocada para o fundo de desenvolvimento DAPS, que será destinado à promoção e ao desenvolvimento e sustento do projeto a longo prazo.

A estrutura de emissões e taxas dará desta forma:
1050 DAPS emitidas por bloco de PoS;
50 DAPS para o fundo de desenvolvimento;
900 DAPS para serem divididos entre o nó de Prova de Serviço (PoS - carteira) que cunhou o bloco e os Masternodes, através do sistema de recompensas em gangorra. Assim, considerando a proporção 60% nós e 40% masternodes na rede, teríamos 540 DAPS para a carteira (staking) e 360 DAPS para masternodes;
100 DAPS serão destinados ao minerador de Prova-de-Auditoria (PoA), para auditarem os blocos.
O "Sistema de Recompensas em Gangorra" é um método pelo qual a rede equilibra a porcentagem da recompensa paga aos nós de staking e Masternodes (MN).
Se houver 1000 MNs e 1000 nós de staking (carteiras), por exemplo, o sistema verá isso como igual e manterá o sistema See-Saw 60%-40% a favor dos Masternodes. Isso porque eles investiram 1 milhão de DAPS para garantir seu Masternode.

Se o número de nós subir drásticamente na direção de mais Masternodes, a rede reequilibrará a equação em 40%-60%, desta vez favorecendo os nós de staking (carteiras).

Isso garantirá a integridade de longo prazo da rede ao equilibrar as recompensas Masternode x staking, evitando o crescimento descontrolado de Masternodes.

ESPECIFICAÇÕES DAPS TOKEN:

Token ERC-20
Fornecimento: 60,000,000,000 DAPS
Distribuição: via AIRDROP

ESPECIFICAÇÕES DAPS COIN:

Fornecimento Inicial: 60,000,000,000 DAPS;
Fornecimento total: 60,000,000,000 [inicial]+10,000,000,000 [emissões] DAPS;
Consenso: Prova-de-Auditoria, Prova-de-Serviço v3, Masternodes (Gangorra);
Técnicas de privacidade: baseada em Secp256k1, Ring Signature, RingCT, e range proof Bulletproof;
Tempo de Bloco: 1 minuto;
Recompensas por Bloco: Consulte Emissões acima
Confirmações para gastar: 4 blocos
Maturação para stakes: 100 blocos
Emissões aproximadas: ~551 milhões de DAPS por ano até alcançar 10 bilhões de DAPS emitidas (~18 anos)

ESPECIFICAÇÕES DA REDE DAPS:

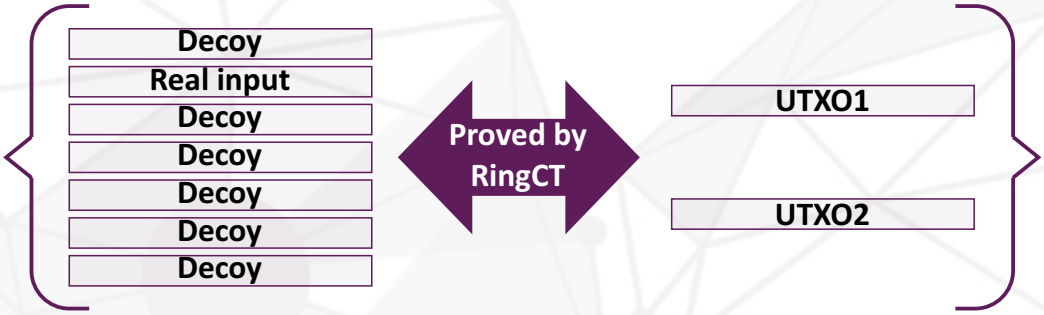
RINGCT

RingCT ou "Ring Confidential Transaction" é uma maneira de misturar uma transação real com um número predeterminado de transações falsas. O tamanho do anel (ring) determina o número de transações falsas que são adicionadas.

Isso significa que a transação real está escondida dentro de uma mistura de transações falsas e, portanto, a transação real e seus valores são muito mais difíceis de discernir.

Enquanto o Monero implementou um tamanho de anel fixo - atualmente 11 - DAPS terá um tamanho de anel gerado aleatoriamente por transação dentro de um determinado intervalo (6 a 12). Isso permite que a rede seja ainda mais segura, garantindo que o usuário não selecione sempre o mesmo tamanho, criando assim a possibilidade de rastreabilidade por meio do hábito.

Enquanto as Ring Signatures ocultam os UTXOs verdadeiros usados para iniciar transações (veja a figura a seguir) e detectam qualquer gasto duplo, o RingCT permite que os nós da rede comprovem que a soma dos valores de entrada de transação são iguais à soma dos valores UTXO mais a taxa de transação. Isso é importante porque todos os valores de transação no DAPS são ocultos por padrão e existem apenas na forma criptográfica Pedersen commitments. O RingCT não exige a revelação dos valores das transações, enquanto ainda é capaz de provar que as somas nos lados de entrada e saída são iguais. A figura a seguir mostra como o Ring Signature e o RingCT são usados juntos.UTXO1



ESPECIFICAÇÕES DA REDE DAPS:

BULLETPROOFS

Bulletproofs são provas curtas de conhecimento zero não interativas que não exigem configuração confiável. O Bulletproof pode ser usado para convencer um verificador de que um texto simples criptografado é bem formado. Por exemplo, provar que um número criptografado está em um determinado intervalo, sem revelar nada sobre o número. Em comparação com os SNARKs, os Bulletproofs não exigem configuração confiável. Entretanto, verificar um Bulletproof consome mais tempo do que verificar uma prova SNARK.

Os Bulletproofs são projetados para permitir transações confidenciais eficientes em Bitcoin e outras criptomoedas. Transações confidenciais ocultam o valor que é transferido na transação. Toda transação confidencial contém uma prova criptográfica de que a transação é válida. As Bulletproofs reduzem o tamanho do arquivo criptográfico de mais de 10kB para menos de 1kB. Além disso, Bulletproofs suportam a agregação de prova, de modo que provar que m valores de transação são válidos adiciona apenas O (log (m)) elementos adicionais ao tamanho de uma única prova. Se todas as transações com Bitcoin fossem confidenciais e o Bulletproof tivesse sido usado, usadas, o tamanho total do conjunto UTXO seria de apenas 17 GB, comparado a 160 GB usados atualmente.

DAPS usa Bulletproofs como provas de intervalo para comprovar que os valores contidos nas transações são positivos. Isso é crítico porque o secp256k1 funciona com um número de espaço de círculo e não há como um nó verificar se os valores codificados são sempre positivos. Sem Bulletproofs verificando se os valores de transação são positivos, um invasor pode criar uma transação com um UTXO com valor positivo enorme enquanto o outro UTXO tem um valor negativo e a soma desses dois valores mais taxas de transação igual à soma das entradas, que resultariam em passar por cima da verificação do RingCT.

ESPECIFICAÇÕES DA REDE DAPS:

ENDEREÇOS SECRETOS

Endereços secretos, assim como as transações secretas, são outro pilar da DAPS.
Enquanto endereços padrão são relativamente fáceis de ler e podem ser facilmente identificados como:3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy

Endereços Secretos da DAPS são bastante diferentes. Segue um exemplo de um endereço público DAPS:
41k8JcYj2EG4eDHbpPNneDdKvFqHFpQNMMGykRUorNnihiY4RaRNdLiUUfThfzugo5auHkq ThwQgZ3EixmxyoDkj17c7Qy6BVWP

Nós chamamos estes endereços de "contas de privacidade". Alguém poderia argumentar que, se esse endereço é público, como o anonimato é alcançado?

Na DAPS, se um remetente quiser enviar um montante para um destinatário, o endereço público do destinatário será usado para gerar uma chave / endereço público gerado uma única vez, baseado em uma chave pública de transação gerada pelo remetente por UTXO.

A particularidade deste esquema é que, ao gerar essa chave pública gerada uma única vez, o remetente não tem como gerar a chave privada correspondente para resgatar o UTXO posteriormente. Essa chave privada será derivada apenas do proprietário do endereço público, que possui os dois pares de chaves privadas em nosso sistema de chaves duplas explicado abaixo.

SISTEMA DE CHAVES PÚBLICAS DUPLAS DAPS

DAPS usa um sistema de chave dupla, fornecendo endereços sigilosos com objetivo de ofuscar endereços. Um endereço público é derivado de um par de chaves exibição e gastos privados. Um endereço público pode conter, opcionalmente, o ID de pagamento, que geralmente é usado pelas exchanges.

DAPS usa a curva secp256k1 do EC para derivar chaves públicas das chaves privadas correspondentes.

Campo	Descrição
Cabeçalho	Comprimento de 1 byte. Cabeçalho = 19 se for um endereço integrado, caso contrário cabeçalho = 18
Chave Pública de Gastos	Chave pública de gastos em formato compactado, cujo comprimento é de 33 bytes.
Chave de Exibição Pública	Chave de exibição pública em formato compactado, cujo comprimento é de 33 bytes.
ID de Pagamento	Campo de 8 bytes usado pelas exchanges para reconhecer transações de diferentes usuários
Verificação de Soma	4 primeiros bytes do hash dos campos acima

ESPECIFICAÇÕES DA REDE DAPS:

O endereço público é codificado no formato base58 para cada bloco de 8 bytes do endereço público da seguinte maneira:

- Endereço público normal: 71 bytes, divididos em oito blocos de 8 bytes e um único bloco de 7 bytes. Cada bloco de endereço é codificado no formato base58, resultando em 11 caracteres base58 por bloco de endereço => 99 caracteres Base58
- Endereço integrado: 79 bytes, divididos em nove blocos de 8 bytes e um único bloco de 7 bytes, resultando em 110 caracteres Base58.

TRANSAÇÕES FURTIVAS

O endereço público/endereço integrado do receptor para uma transação deve ser enviado ao remetente, cuja carteira realiza as seguintes etapas para criar uma transação totalmente privada:

- Análise do endereço público para extrair a chave de visualização pública Pv, a chave de gasto público Ps e a ID de pagamento (opcional) do destinatário;
- Verificar se a carteira tem saldo suficiente para enviar;
- Gerar uma chave pública P gerada uma vez para o receptor da seguinte forma:
  - Gerar uma chave privada de transação Ts e sua chave pública de transação correspondente Tp
  - P = H (Ts * Pv) * G + Ps onde:
    - H é uma função hash;
    - * e + são a multiplicação e adição na curva secp256k1;
    - G é o ponto gerador base na curva secp256k1;
  - Uma chave pública gerada uma vez é gerada por transação de saída na transação que está sendo feita. Cada transação de saída tem uma chave privada de transação diferente para evitar fundos não resgatáveis com assinatura de anel descrita abaixo;
- Criar uma transação de saída com destino como a chave pública gerada pelo tempo acima e o valor de envio esperado;
  - Criar um Pederson commitment para a transação de saída;
  - Gerar curva elíptica DiE Hellman secreta ECDHS;
  - Codificar o montante da transação de saída com o segredo do ECDHS;
  - Gerar bulletproof para o montante da transação de saída;
- Selecionar um conjunto de UTXO gastável para serem transações de entrada;
  - Calcular a taxa de transação com base em uma taxa estimada;
  - Calcular o troco = Soma das transações de entrada-quantidade enviada-taxa de transação;
  - Tornar a taxa de transação explícita na transação;
  - Gerar imagens da chave e colocá-as na transação de entrada;
- Gerar Ring Signature;
  - Gerar o tamanho aleatório do anel Ring _Size (6-12);
  - Para cada transação de entrada, selecione Ring _Size iscas;
  - Calcular assinaturas de anel multi-chaves com base no Monero, RingCT, e Ring signature.

MASTERNODES E STAKING NODES DA DAPS

Em sistemas baseados em Masternodes, como o PIVX, os Masternodes são recompensados por fornecer serviços adicionais, como "envio instantâneo", e as recompensas são enviadas para o endereço que contém as moedas como garantia. Se tal mecanismo fosse usado na DAPS, os fundos para Masternodes seriam perdidos porque as assinaturas de anel detectariam ou marcariam uma transação como gasto duplo, mesmo se dois UTXOs diferentes do mesmo endereço fossem gastos na transação. Isso significa que apenas uma das recompensas do UTXO do Masternode pode ser resgatada se as recompensas forem enviadas para o mesmo endereço.

DAPS é projetado para que este mecanismo de incentivo de Masternodes gere um novo endereço/chave pública toda vez que o Masternode for recompensado. DAPS faz isso ao exigir que os usuários forneçam o endereço público (o endereço longo) para a transação de garantia (1M). O endereço público do Masternode será colocado na fila de pagamento. Durante a criação de um bloco PoS, um nó de staking (carteira), então, pegará um dos endereços públicos na fila e gerará uma chave pública gerada uma única vez para o pagamento do Masternode. Isso irá garantir que os UTXOs das recompensas dos Masternodes serão todos “gastáveis”.

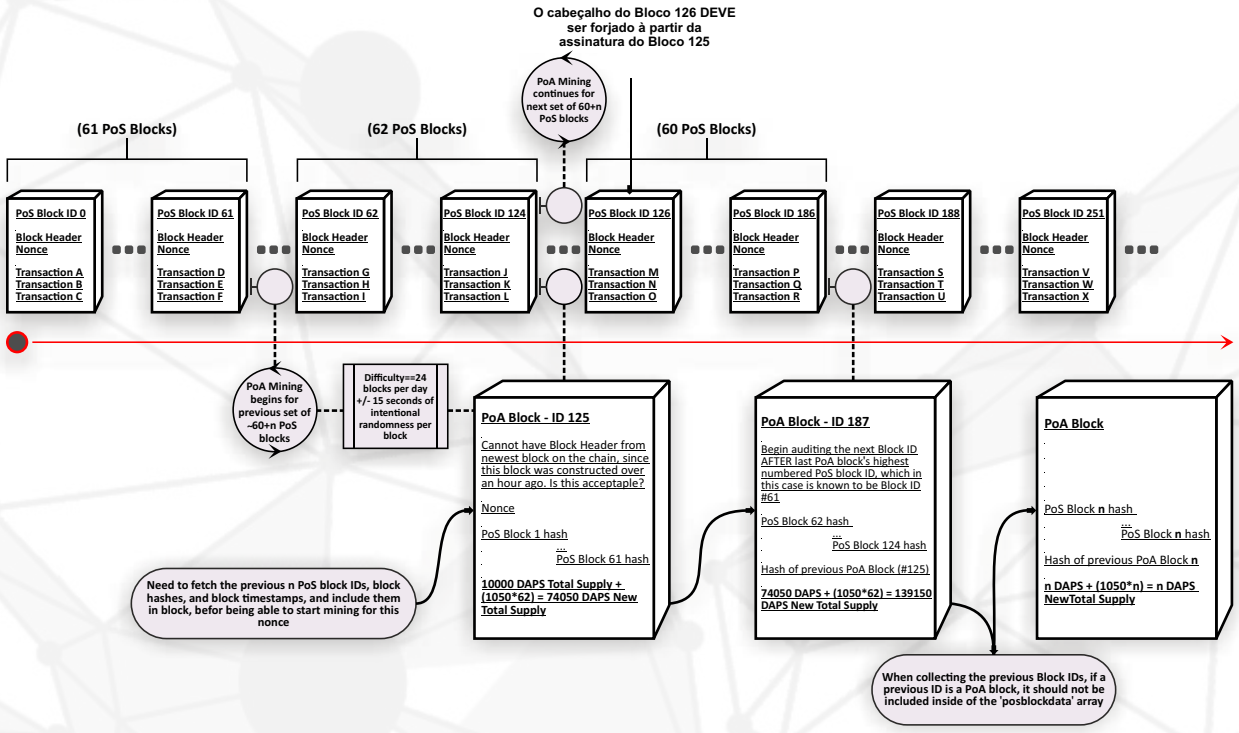
Esse mecanismo também é aplicado ao nó de staking (ou carteiras), enquanto cria blocos PoS, para garantir que todas as recompensas de staking sejam enviadas para chaves públicas diferentes.

CONSENSO PoA E PoS - DETALHES

1. No PoA block shall be accepted onto the chain unless at least 59-60 minutes have elapsed since the timestamp of the previously accepted PoA block. *This should ensure that PoA blocks remain spaced out across the chain and cannot end up back-to-back-to-back for any reason.*
2. A PoA block must contain the hash of the previous PoA block, thus forming a continuously stranded sub-chain-of-PoA-blocks.
3. A PoA block must not include another PoA block's hash, height, or timestamp in its own `posblocksaudited` array.
4. Every block hash included in posblocksaudited must be a valid hash of a PoS block that can currently be seen on the chain.
5. Every block timestamp included in posblocksaudited must be from a time that is earlier than the PoA block's own timestamp. No PoA block is allowed to audit blocks that have occurred after itself.
6. A PoA block is not allowed to audit a PoS block hash that another PoA block has already audited.

A PoA block can be added to the chain at any time. This allows for PoS blocks to carry on with their minting process uninhibited, and a PoA block would have to select a certain number of existing, sequential PoS blocks to audit, make a record of their block IDs + block hashes + timestamps as a relational list ordered by block ID, and then add itself to the chain as the next block ID in line.

Future PoA blocks look up the previous PoA's block ID, look inside it for the highest numbered PoS block ID, and then begin their audit process, taking into account that if any of those block IDs are a PoA block, they should be ignored.



«Privacidade é um direito, não um privilégio»

TOR/OBFS4

Versões anteriores deste whitepaper mencionavam o uso de TOR e OBFS4. Após uma extensa investigação, tomamos a decisão de excluí-los da nossa tecnologia por hora.
As razões para isso são simples, mas carregam um peso significativo.
O TOR é bloqueado por muitos provedores de serviços de Internet globalmente, exigindo procedimentos de configuração extensivos para estabelecer "pontes" de comunicações, o que pode levar muitas pessoas a não quererem utilizar o DAPS devido a uma grande barreira de entrada.
Outra questão relacionada a provedores e TOR é que muitos provedores - ao ver alguém usando TOR, independentemente do motivo - irão solicitar a pessoa a não fazê-lo novamente, caso contrário sua conta pode ser suspensa ou simplesmente fechada sem aviso prévio. De qualquer maneira, isso é ruim e às vezes pode até terminar com uma visita de órgãos da Lei. E isso não é algo que desejamos para nossos usuários.

Continuamos investigando o TOR em maior profundidade e o consenso geral é que podemos introduzir o TOR como "opcional" em uma versão futura.
Como esses são sistemas periféricos, a blockchain não precisará ser redefinida, dividida ou bifurcada para implementação.

OUTRAS CARACTERÍSTICAS

- Emissões estáticas: sem modelos extravagantes de inflação, emissões uniformes;
- Blocks de até 2 MB;
- Masternodes: Incentivados 24/7 e que podem ser usados para recursos avançados;
- Multinodes: vários masternodes por máquina. Chega de spam de servidores!

Usando os recursos de blockchain acima, esperamos ofuscar completamente transações, endereços, saldos e nós/IP. Com uma auditoria interna própria de fornecimento de moeda na blockchain, o sistema será “sem confiança” e evitará os problemas com a questão da "confiança" das moedas totalmente privadas existentes. Essa mistura única de recursos baseados em uma rede de staking será chamada de Protocolo de Harpócrates e acreditamos que isso mudará o padrão das moedas de privacidade. Acreditamos, também, que o Proof-of-Audit pode aumentar e aprimorar outros protocolos contemporâneos, tornando a missão do nosso projeto benéfica para a indústria como um todo.

- DAPS Ecossistema & Mundo: Iniciativas serão empreendidas para incorporar o DAPS com uso real e utilidade para estimular a adoção em massa.

OBSERVAÇÕES:

Por favor, note que este documento não é um prospecto de propaganda. Foi constituído apenas para fins informativos, para apresentar o projeto DAPS Coin à partir de 2019.

Esteja ciente de que nenhuma compra é necessária. Você é livre para participar do projeto ou não. É da sua responsabilidade conhecer as leis existentes no seu país antes de comprar ou aderir ao projeto DAPS. Você deve ler, entender e aceitar os termos deste documento antes de se envolver no projeto.

Especificações e informações técnicas estão sujeitas a alterações. A equipe DAPS realizou uma fase de testes de sucesso em março de 2019.

DAPS passará por uma auditoria de código de terceiros antes do lançamento da sua blockchain.

DOCUMENTAÇÃO:

Bitcoin trustless

Z-cash Trust Problem

Libzerocoin Protocol

DAP Protocol, by Sasson et al

Masternodes

Masternodes

See-saw reward scheme

Posv3

Ring CT

Bulletproofs

Stealth Addresses